УДК 004.724.4(045)

[1]**Ю.О. Кулаков**, д.т.н., проф.
[2]**В.В. Лукашенко,** к.т.н., доц.
[3]**А.В. Левчук,** старш. інсп.

# СПОСІБ ОРГАНІЗАЦІЇ БАГАТОШЛЯХОВОЇ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В БЕЗПРОВОДОВІЙ МЕРЕЖІ MPLS

[1]Національний технічний університет України «Київський політехнічний інститут»
[2, 3]Національний авіаційний університет
[3]E-mail: LevchukAlla@yandex.ru

*Запропоновано спосіб організації, багатошляхової безпечної маршрутизації в безпроводовій мережі MPLS, що дозволить значно поліпшити швидкість обробки інформації та захистить трафік, який передається.*

**Ключові слова:** безпечна маршрутизація, багатошляхова маршрутизація, мережа MPLS.

## Вступ

Існуючі методи багаторівневої маршрутизації в мобільних комп'ютерних мережах спрямовані на підвищення якості передачі інформації і забезпечення рівномірного завантаження комп'ютерної мережі і, як правило, не забезпечують необхідного рівня захисту інформації.

Безпроводові технології мають принциповий недолік відносно безпеки – доступ до безпроводового середовища передачі даних не складає особливих труднощів. Відомі методи підвищення безпеки переважно орієнтовані на мережі з фіксованою структурою.

## Аналіз існуючих рішень

Наявність безпроводових каналів зв'язку спрощує доступ до інформації, що передається, це вимагає додаткових вимог до задачі забезпечення інформаційної безпеки інформації. Ефективність функціонування безпроводових мереж значною мірою залежить від вирішення задачі маршрутизації. У зв'язку з цим рішення завдання ефективної безпечної маршрутизації є актуальною в безпроводових комп'ютерних мережах.

Одним із підходів до вирішення завдання безпечної маршрутизації є протоколи маршрутизації, які вирішують проблеми безпеки в безпроводових мережах, ґрунтуючись на певних припущеннях і вимогах.

У роботі [1] наведено результати порівняння різних протоколів безпечної маршрутизації, на підставі яких можна зробити висновок, що більшість цих протоколів вимагають наявності третього online-сервера, який:

– бере участь у підтвердженні прав доступу;
– служить для полегшення збору, перевірки справжності відкритих ключів.

Під цю категорію потрапляють такі протоколи:

– ARAN;
– SAD;
– SEAD;
– SAODV.

Крім того, захищений протокол маршрутизації за запитом Resilient to Byzantine Failures вимагає наявності закритих ключів на всіх вершинах шляху від вершини-відправника до вершини-приймача.

Кожна проміжна вершина використовується для підтвердження прийому прийнятих пакетів. Як альтернативне рішення застосовуються протоколи SAR та IPsec, які використовують заздалегідь розраховані дані, що приховуються кожним вузлом, для обміну повідомленнями між кожною парою вершин.

Більшість протоколів маршрутизації призначені для забезпечення коректності маршрутизації, деякі з них вирішують проблеми некоректної поведінки вузла і способи виявлення вторгнення. Але майже жодна зі схем не розглядає питання забезпечення безпеки даних, які передаються.

**Мета** роботи – запропонувати спосіб використання багатошляхової безпечної маршрутизації.

**Постановка завдання**

Для вирішення завдання безпечної передачі даних пропонується організувати багатошляхову маршрутизацію на базі технології MPLS, що дозволить забезпечити побудову магістральних мереж, що мають:

– майже необмежені можливості масштабування;

– підвищену швидкість обробки трафіка;

– безпрецедентну гнучкість щодо організації додаткових сервісів.

Мітка – це короткий ідентифікатор фіксованої довжини, який визначає клас FEC [2].

Головними перевагами технології багатопротокольної комутації за мітками порівняно з традиційною маршрутизацією є:

– відокремлення вибору маршруту від аналізу IP-адреси, що дає можливість надавати широкий спектр додаткових сервісів при збереженні масштабованості мережі;

– збільшення швидкості обробки пакетів у вузлах, оскільки не потрібно «витягувати» пакет із кадру, визначати IP-адресу та здійснювати пошук у таблиці маршрутизації найбільш відповідного адресного префікса;

– гнучка підтримка якості обслуговування (QoS), інтегрованих сервісів і віртуальних приватних мереж;

– можливість використовувати для прийняття рішень про маршрутизацію не лише адреси одержувача, а й інших даних, наприклад, адреси відправника, вимог щодо якості обслуговування і т.д.;

– розподіл функціональності між ядром і граничною областю мережі, за рахунок чого може бути спрощена структура маршрутизаторів ядра мережі та підвищена їх швидкодія;

– політика керування трафіком може бути реалізована тільки на граничних маршрутизаторах, що полегшує її налаштування.

**Вирішення завдання**

В основі мережі MPLS (рис. 1) лежить принцип обміну міток [3].

Мітка передається в складі будь-якого кадру, причому спосіб її прив’язки до кадру залежить від використовуваної технології канального рівня.

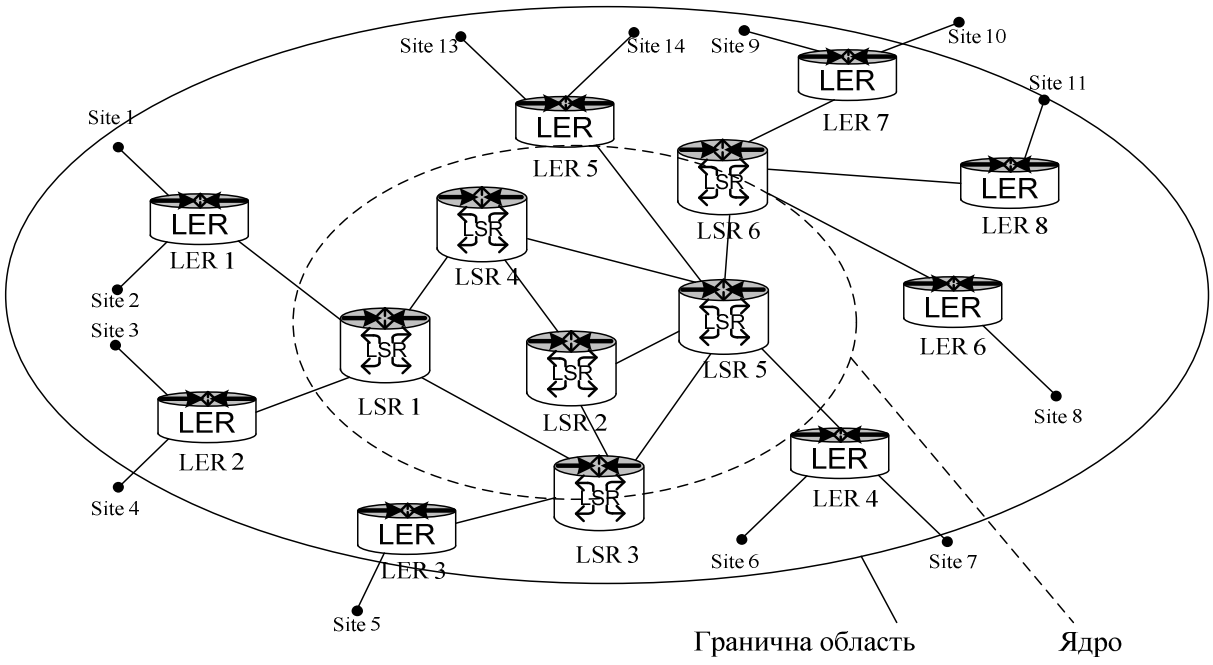


Рис. 1. Мережа MPLS

За значенням мітки пакета визначається його приналежність до певного класу на кожній із областей комутованого маршруту.

Мережа MPLS ділиться на дві функціонально різні області – ядро і граничну область (рис. 1).

До ядра відносяться маршрутизатори LSR1...LSR6, а до граничної області – LER1...LER8.

Мережі або окремі вузли site1...site14 не використовують технологію комутації за мітками, але використовують мережу MPLS як опорну (звичайно це вузли або мережі користувачів).

Інтенсивні обчислення припадають на граничну область, а високопродуктивна комутація виконується в ядрі, що дозволяє оптимізувати конфігурацію пристроїв MPLS залежно від їхнього місця розташування в мережі.

Мережі MPLS організують помічені комутовані маршрути (LSP) для проходження даних по мережі.

Маршрути LSP визначаються послідовністю міток, призначених вузлів на шляху проходження пакета від джерела до одержувача.

Маршрути LSP направляють пакети одним із двох варіантів [4]:

– послідовна маршрутизація (по ділянках);

– явна (точно визначена) маршрутизація.

**Послідовна маршрутизація**

У випадку послідовної маршрутизації кожний маршрутизатор MPLS незалежно вибирає наступну транзитну ділянку для заданого класу еквівалентності (рівноцінності) передачі (FEC). FEC описує групу пакетів одного типу. Усі пакети присвоєного класу FEC отримують один режим маршрутизації.

**Явна маршрутизація**

У випадку явної маршрутизації завчасно визначається весь перелік вузлів, через які проходить LSP.

Певний маршрут може бути оптимальним чи ні, але він ґрунтується на уявленні мережевої топології і потенційно на додаткових обмеженнях. Цей спосіб називається маршрутизацією з обмеженнями (Constraint-Based Routing). Щоб гарантувати QoS, ресурси на маршруті можуть резервуватися. Це дозволить розгорнути в мережі процес формування трафіку для оптимізації використання пропускної здатності мережі.

Для організації та оповіщення мережі кожен маршрутизатор MPLS будує інформаційну базу міток (LIB) – таблицю, в якій визначається, як передавати пакет. Ця таблиця пов’язує кожну мітку з відповідним FEC і вихідним портом, на який буде передаватися пакет. Ця LIB зазвичай створюється на додаток до таблиці маршрутизації та інформаційної бази передачі (FIB), які обслуговують традиційні маршрутизатори.

Хмара мережі MPLS складається з маршрутизаторів комутації за мітками і фізичних каналів зв’язку між ними. У мережі може використовуватися будь-який протокол канального рівня, а також будь-який протокол мережевого рівня.

Безліч шляхів LSP і маршрутизаторів LSR являють собою віртуальну топологію, організовану поверх фізичної мережі. При цьому різні шляхи LSP можуть розділяти одні й ті ж фізичні канали передачі даних між маршрутизаторами LSR.

Функціональну схему блоку розподілу трафіку, розташованого у вхідному вузлі показано на рис. 2.

Цьому механізму не потрібна статистика вимог трафіку або інформація про стан потоку. У процедурі розподілу трафіку визначається, як і коли перемикати трафік між LSP. Це робиться на основі статистики LSP, яка виходить із вимірів з використанням тестових пакетів. Процедура розподілу трафіку складається з двох етапів:

– етап моніторингу;

– етап балансування навантаження.

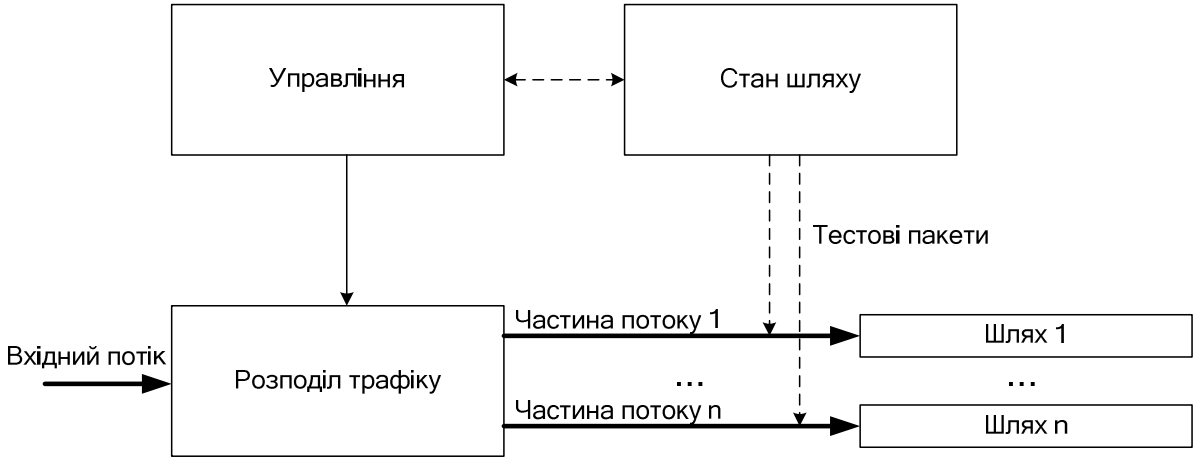


Рис. 2. Схема блоку розподілу трафіку у вхідному вузлі

На етапі моніторингу в разі виявлення значної і постійної зміни стану мережі виконується перехід на етап балансування.

На етапі балансування алгоритм намагається вирівняти навантаження серед LSP. Як тільки навантаження вирівнюється, алгоритм переходить на етап моніторингу і весь процес повторюється.

У роботі [5] запропоновано два способи розділення трафіку:

– жорсткий розподіл;

– оптимальний розподіл.

Жорсткий розподіл розділяє секретне повідомлення на стільки частин, скільки знайдено оптимальних шляхів:

$$N = \frac{N_{\text{ч}}}{N_p},$$

де $k$ – жорсткий розподіл;

$N_{\text{ч}}$ – кількість частин повідомлення;

$N_p$ – кількість шляхів що не перетинаються.

Під оптимальними шляхами розуміється безліч шляхів, що не перетинаються.

Оптимальний розподіл дає можливість розподілу переданого повідомлення на оптимальну кількість частин. По одному маршруту може бути передано кілька частин залежно від завантаженості каналу зв'язку:

$$k_{\text{opt}} = \frac{N_{\text{ч}}}{N_{p\ \text{opt}}},$$

де $k_{\text{opt}}$ – оптимальний розподіл;

$N_{p\ \text{opt}}$ – кількість оптимальних шляхів.

З урахованням розміру вхідного повідомлення запропоновано використовувати два способи:

– за необхідності передачі повідомлення великого розміру потрібно використовувати жорсткий розподіл, оскільки рівномірно будуть завантажені всі канали зв'язку;

– якщо повідомлення невеликого розміру, тоді повідомлення ділиться на оптимальну кількість частин і формується потрібна кількість шляхів, за якими буде здійснюватися багатошляхова маршрутизація.

Припустимо, що $C(x)$ – функція вартості використання каналу. Як вартість може виступати, наприклад, затримка при передачі пакетів, фінансова вартість використання каналу і т.д. Задача розподілу трафіка визначається так:

$$\min_x C(x) = \sum_l C_l(x^l).$$

За умови

$$\sum_{p \in P_S} x_{sp} = r_s$$

для всіх $s \in S$,

де $P_s$ – множина всіх шляхів *LSP*;

$x_{sp}$ – частина трафіку, що передається по шляху $p$;

$r_s$ – потік трафіку між вхідним і вихідним вузлом.

Сума потоків даних, що проходять по каналу, визначається так:

$$x^l = \sum_{s \in S} \sum_{l \in p, p \in P_S} x_{sp}.$$

Сума потоку даних, що проходять по каналу l , визначається так:

$$\frac{\partial C}{\partial x_{sp}}(x) = \sum_{l \in P} C_l'(x^l).$$

У роботі [5] доведено, що вектор значень *x* даватиме мінімальне значення функції вартості *C(x)* тоді і тільки тоді, коли трафік поділяється між шляхами *LSP*, значення похідної функції $\frac{\partial C}{\partial x_{sp}}(x)$ будуть мінімальними і, отже, рівними.

При послідовному наближенні *x* до оптимального значення на кожному кроці ітерації *x* буде приймати такі значення:

$$x(t+1) = [x(t) - \gamma \nabla C(t)],$$

де $\gamma > 0$ – це крок, який повинен бути обраний досить маленьким;

$\nabla C(t)$ – це вектор, де кожен елемент для шляху *p* в часі *t* визначається так:

$$[\nabla C(t)]_{SP} = \frac{\partial C}{\partial x_{SP}}.$$

Алгоритм закінчується, коли

$|x(t+1)-x(t)|<e$.

Результат роботи безпроводової мережі MPLS з використанням удосконаленого алгоритму передачі даних на першому шляху показано на рис. 3.

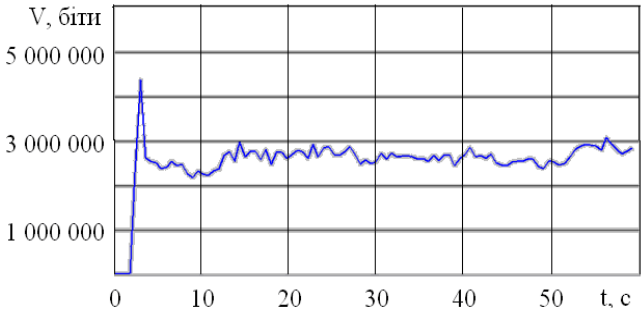


Рис. 3. MPLS з модифікацією алгоритму на LER4

## Висновки

Запропоновано спосіб організації багатошляхової маршрутизації, який дозволить збільшити швидкість обробки інформації і з максимальним ступенем захисту убезпечити трафік, який передається.

## Література

1. *Кулаков Ю.А.* Проблеми інформатизації та управління / Ю.А. Кулаков, А.О. Деревянчук // Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей: зб. наук. пр. – К.: НАУ-друк, 2009. – № 3(27). – С. 99–103.

2. *Lasserre, M.; Kompella, V.* 2005. Virtual Private LAN Services over MPLS. – L2VPN Working Group. 500 p.

3. *Шиллер Й.* Мобильные коммуникации / Шиллер Йоган / пер. с англ. – М.: Вильямс, 2002. – 384 с.

4. *Кулаков Ю.А.* Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности / Ю.А. Кулаков, В.В. Лукашенко, А.В. Левчук // Защита информации. – 2011. – № 2 (51). – С. 120–126.

5. *Nagaratnam, N.; Janson, P.; Dayka, J.; Nadalin, A.; Siebenlist, F.; Welch, V.; Foster, I.; Tuecke, S.* 2003. The Security Architecture for Open Grid Services. 368 p.

Стаття надійшла до редакції 18.07.2011.